UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/539,648	12/17/2007	John Owlett	GB920020055US1	6660

30449 7590 08/18/2009

SCHMEISER, OLSEN & WATTS
22 CENTURY HILL DRIVE
SUITE 302
LATHAM, NY 12110

EXAMINER	
WOLDEMARIAM, NEGA	
ART UNIT	PAPER NUMBER
2433	

MAIL DATE	DELIVERY MODE
08/18/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/539,648	OWLETT ET AL.	
	Examiner	Art Unit	
	NEGA WOLDEMARIAM	2433	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 December 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-26* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-26* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *17 December 2007* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☒ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *10/01/2007, 06/15/2005*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to: an original application filed on December, 17 2007.

2. Claims 1—26 are currently pending. Claim 1, 22, 24, and 25 are independent claims.

3. There is no IDS submitted with this application.

Priority

Acknowledgment is made of applicant's claim for foreign priority based on an application filed in United Kingdom on December, 21 2002. It is noted, however, that applicant has not filed a certified copy of the foreign application as required by 35 U.S.C. 119(b).

Acknowledgment is made of applicant's claim for priority under 35 U.S.C. 119(a)-(d) based upon an application filed in United Kingdom on December, 21 2002. A claim for priority under 35 U.S.C. 119(a)-(d) cannot be based on said application, since the United States application was filed more than twelve months thereafter.

Information Disclosure Statement

The information disclosure statement filed 06/15/2005 fails to comply with the provisions of 37 CFR 1.97, 1.98 and MPEP § 609 because “E-Signature Solutions, DataCert.com, 9 pgs" does not dated. It has been placed in the application file, but the information referred to therein has not been considered as to the merits. Applicant is advised that the date of any re-submission of any item of information contained in this information disclosure statement or the submission of any missing element(s) will be the date of submission for purposes of determining compliance with the requirements based

on the time of filing the statement, including all certification requirements for statements under 37 CFR 1.97(e). See MPEP § 609.05(a).

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claim1—21, 24 and 26 rejected under 35 U.S.C. 101 because

In summary, Claim 1 recites "*A method for generation a conditional electronic signature*"" comprising steps that may be performed manually and/or mentally. Thus, the recited method is not tied to a particular machine or apparatus. Additionally, none of the recited steps transform a particular article into a different state or thing.

Accordingly, the recited method is nonstatutory subject matter.

Claim 26 recites "A computer program comprising program code instructions "" comprising steps that may be performed manually and/or mentally. Thus, the recited program is not tied to a particular machine or apparatus. Additionally, none of the recited steps transform a particular article into a different state or thing.

Accordingly, the recited method is nonstatutory subject matter.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1—26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sudia et al. US Patent. No.: 5995625 (hereinafter Sudia) and further in view of Koyama et al. US pub. No.: 20020116382 A1(hereinafter Koyama)

As to independent claim 1, Sudia teaches **a method for generating a conditional electronic signature,** (see Sudia col. 3, lines 39—43, In order to verify the CA's signature, the certificate content must be hashed and encrypted with the same conditions and acceptance phrase), **the method comprising the steps of: encrypting the data item, encrypting the one or more conditions separately from the data item** (see Sudi, col. 3, lines 3—8, In these embodiments, the invention includes forming a key value from a combination of an acceptance phrase and an issuing CA policy statement (the conditions); encrypting the subscriber's public key with the key value and then inserting the encrypted public key into the subscriber's certificate), **combining the encrypted data item and the encrypted one or more conditions, and encrypting the combination to generate a digital signature block that inherently represents the data item and the one or more conditions and enables cryptographic verification of both the data item and the one or more conditions** (see Sudi col. 5, lines 56—62, The various digested data (formed at P12, P16 and P20) are then combined by computer 102 using combine function 28 to form a wrap key value 30. That is, the digest of the conditions 14, the digest of the acceptance phrase 20, and, if provided, the digest of the other data 26 (or the other data 22 directly) are then combined using combine function 28 to produce a wrap key value 30 (at P22).) Sudi does not explicitly teach the following **performed in response to one or more conditions being**

specified for an electronic signature of a data item. However Koyama teaches (see Koyama par. [0030], The procedure of creating the change request list is structured by including step S21 of incorporating (integrating) the change request and the utilization information into one item of data, step 22 of providing a digital signature of the user thereinto, and step S23 of performing encryption by using a public key.).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention of Electronic cryptographic packing taught in Sudia to include conditions being specified for an electronic signature of a data item. One of ordinary skill in the art would have been motivated to include utilization restriction information in order to be flexible and diverse in a digital signature application in electronics digital dat see Koyama (paragraphs [00010]).

As to independent claim 22, Sudi teaches **a data processing apparatus for generating conditional electronic signatures** (see Sudia col. 3, lines 39—43, In order to verify the CA's signature, the certificate content must be hashed and encrypted with the same conditions and acceptance phrase), **for encrypting the data item, encrypting the one or more conditions separately from the data item, combining the encrypted data item and the encrypted one or more conditions** (see Sudi, col. 3, lines 3—8, In these embodiments, the invention includes forming a key value from a combination of an acceptance phrase and an issuing CA policy statement (the conditions); encrypting the subscriber's public key with the key value and then inserting the encrypted public key into the subscriber's certificate), **and encrypting the combination to generate a digital signature block that inherently represents the data item and the one or more conditions and enables cryptographic verification of both the data**

item and the one or more conditions (see Sudi col. 5, lines 56—62, The various digested data (formed at P12, P16 and P20) are then combined by computer 102 using combine function 28 to form a wrap key value 30. That is, the digest of the conditions 14, the digest of the acceptance phrase 20, and, if provided, the digest of the other data 26 (or the other data 22 directly) are then combined using combine function 28 to produce a wrap key value 30 (at P22).) Sudi does not explicitly teach the following; **comprising: one or more cryptographic components, responsive to one or more conditions being specified for an electronic signature of a data item** However Koyama teaches (see Koyama par. [0030], The procedure of creating the change request list is structured by including step S21 of incorporating (integrating) the change request and the utilization information into one item of data, step 22 of providing a digital signature of the user there in to, and step S23 of performing encryption by using a public key.) **and means for transmitting to a recipient the data item, the one or more conditions and the digital signature block**(see Koyama par. [0021], A data transmission side can encrypt data by using the public key, and can transmit the encrypted data to the reception side).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention of Electronic cryptographic packing taught in Sudia to include conditions being specified for an electronic signature of a data item. One of ordinary skill in the art would have been motivated to include utilization restriction information in order to be flexible and diverse in a digital signature application in electronics digital data see Koyama (paragraphs [00010]).

As to independent claim 24, Sudi teaches **a method for disseminating status information for conditionally signed data items, wherein the conditionally signed data items include**

executable content for updating a registry in response to one of the conditionally signed data items being forwarded to a recipient or being identified as rejected (see sudi col. 2, lines 18—23, In general, this invention operates on a computer system which includes a computer with a processor (CPU) which executes programs in a memory in a known manner. The computer may also include special purpose hardware such as a DES processor or the like), Sudi does not explicitly teach the following **the registry maintaining a list of recipients of the data item, the method including the steps of:in response to forwarding of the conditionally signed data item to a new recipient, executing the executable content to update the list of recipients in the registry** However Koyama teaches (see Koyama par. [0047], In addition, also when a user terminal A performs re-redistribution of the distribution format data 301 to a user terminal B, the distribution record database 105 can similarly be updated using the creator communication address 311. According to the above, even when the distribution format data 301 is to be redistributed many times, the data creator terminal 101 can update the distribution record database 105 for distribution of revised data. Moreover, revised data can be distributed to all those who preserve the distribution format data 301.); **and in response to an indication that the conditionally signed data item is rejected, executing the executable content to update the registry and disseminating an indication that the data item is rejected to each of the recipients in the registry list** (see Koyama par. [0066] Moreover, also when the user terminal A performs re-redistribution of the distribution format data 301 to the user terminal B, the distribution record database 105 can similarly be updated. According to the above, even when redistributing the distribution format data 301 many times, the management center 501 can

update the center database 505 in each distribution of the revised data. In this way, revised data can be distributed to all those who preserve the distribution format data 301).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention of Electronic cryptographic packing taught in Sudia to include conditions being specified for an electronic signature of a data item. One of ordinary skill in the art would have been motivated to include utilization restriction information in order to be flexible and diverse in a digital signature application in electronics digital data see Koyama (paragraphs [00010]).

As to independent claim 25, this claim is directed to a data processing apparatus executing the method of claim 24; therefore it is rejected along similar rationale.

As to claim 2, the combination of Sudi and Koyama teaches **a method, wherein each of a plurality of specified conditions is separately encrypted and combined with the encrypted data item, and wherein the combination is then further encrypted** (see Sudi, col. 18, lines 35—45, When a signature on a signed transaction or document includes multiple data fields, such as signature attributes as defined in PKCS#7, ANSI X9.45 and elsewhere, it will be clear to one skilled in the art that the wrapping process defined herein can be applied separately to one or more individual fields within the signature block, since the signature block is itself a compound message. In general, digital data to be wrapped can be partitioned in any way and different wrap keys can be formed for any or all of the partitions using the same or different conditions, acceptance phrases and other data for each partition of data).

As to claim 3, the combination of Sudi and Koyama teaches **a method, wherein the encryption of the data item and separate encryption of the conditions are each one-way hashing steps**

to generate verifiable representations of the data item and conditions (see col. 3, lines 40—46, In order to verify the CA's signature, the certificate content must be hashed and encrypted with the same conditions and acceptance phrase. The signed hash appended to the certificate is then verified using the CA's public key and the encrypted hash generated by the user. If the verification computation is successful, then the CA's signature is valid) and (see Koyama par. [0023], The hash conversion is characterized by performing a one-way conversion for producing a specific-sized conversion result with high randomness for data.).

As to claim 4, the combination of Sudi and Koyama teaches **a method,, wherein the step of combining the hashed data item and conditions comprises concatenating the hashed data item and hashed conditions, hashing the product of the concatenation to produce a final digest, and further encrypting the final digest to generate a digital signature block**. (see col. 5, lines, 56—62, The various digested data (formed at P12, P16 and P20) are then combined by computer 102 using combine function 28 to form a wrap key value 30. That is, the digest of the conditions 14, the digest of the acceptance phrase 20, and, if provided, the digest of the other data 26 (or the other data 22 directly) are then combined using combine function 28 to produce a wrap key value 30 (at P22).)

As to claim 5, the combination of Sudi and Koyama teaches **a method, wherein the step of encrypting the combination uses an encryption method for which the result of (a) combining the encrypted data item and the encrypted one or more conditions and then encrypting the combination differs from a result of (b) encrypting both the encrypted data item and the encrypted one or more conditions and then combining the doubly encrypted data item and conditions** (see Sudi col. 5, lines 56—61, The various digested data (formed at

P12, P16 and P20) are then combined by computer 102 using combine function 28 to form a wrap key value 30. That is, the digest of the conditions 14, the digest of the acceptance phrase 20, and, if provided, the digest of the other data 26 (or the other data 22 directly) are then combined using combine function 28 to produce a wrap key value 30 (at P22)).

As to claim 6, the combination of Sudi and Koyama teaches **a method, wherein the encryption method implements Cipher Block Chaining encryption** (see Sudi, col. 17, lines 8—13, When recording the glyph value, UID, and buyer identification in the database, the seller may protect the integrity of those database entries by a method of hash chaining, such as by including a hash of the previous database record in the current one, and then including a hash of the current record in the next record, and so on, as is known in the prior art).

As to claim 7, the combination of Sudi and Koyama teaches **a method, wherein the encryption of the data item and separate encryption of the conditions each use Cipher Block Chaining encryption methods** (see Sudi, col. 17, lines 8—13, When recording the glyph value, UID, and buyer identification in the database, the seller may protect the integrity of those database entries by a method of hash chaining, such as by including a hash of the previous database record in the current one, and then including a hash of the current record in the next record, and so on, as is known in the prior art).

As to claim 8, the combination of Sudi and Koyama teaches **a method**, **wherein the step of encrypting the combination to generate a digital signature block uses a private key of a public/private key cryptographic solution to produce a conditional signature** (see Koyama par. [0031], In the present embodiment, an assumption is made that a public key 1 and a private

key 1 are allocated to the data creator, and a public key 2 and a private key 2 are allocated to the user.).

As to claim 9, the combination of Sudi and Koyama teaches **a method, wherein the step of encrypting the combination to generate a digital signature block uses a symmetric key of a symmetric-key cryptographic solution to produce a conditional signature** (see Sudi col. 3, lines 12—15, The encryption is preferably performed using a symmetric encryption algorithm such as DES or the like. Accordingly, the wrap and unwrap key values are generally the same).

As to claim 10, the combination of Sudi and Koyama teaches **a method, including the step of transmitting to a recipient the data item** (see Koyama par. [0021], A data transmission side can encrypt data by using the public key, and can transmit the encrypted data to the reception side), **the one or more conditions and the digital signature block, such that a recipient, who has access to the cryptographic processes used for performing the encrypting steps and has access to a corresponding decryption key** (see Koyama par. [0036], Using the private key 2 preset for the per-user in the user terminal 201, the conversion unit 211 decrypts the encrypted distribution format data 301. The determination unit 208 performs a hash conversion for the utilization restriction information 303, and compares the conversion result to the hash value 304), **is enabled to: decrypt the digital signature block to produce a first result** (see Koyama par. [0038], Then, the encrypted data 313 in the distribution format data 301 is decrypted using the data encrypting key 308 (secret key 1) in the distribution format data 301, and the data is displayed);**encrypt the data item, encrypt the one or more conditions separately from the data item, and combine the encrypted data item and encrypted one or more conditions to produce a second result; and compare the first and second results to determine whether**

they match (see Sudi, col. 5, lines 56—62, The various digested data (formed at P12, P16 and P20) are then combined by computer 102 using combine function 28 to form a wrap key value 30. That is, the digest of the conditions 14, the digest of the acceptance phrase 20, and, if provided, the digest of the other data 26 (or the other data 22 directly) are then combined using combine function 28 to produce a wrap key value 30 (at P22).).

As to claim 11, the combination of Sudi and Koyama teaches **a method, including transmitting the encryption algorithms to the recipient** (see Sudi col8, lines 4—11, Generally, cryptographic certificate 38 has various fields, including certificate number 40, the name of the issuing CA 42, the subscriber's name 44, an algorithm identifier 46, the subscriber's public key 48, an extension phrase 50, an extension policy (a policy identifier) 52, a validity period 54, other general information 56 and other cryptographic, key-related information 58. The certificate 38 is digitally signed by the issuing CA and carries the CA's signature 60).

As to claim 12, the combination of Sudi and Koyama teaches **a method, including transmitting to the recipient the interim results of each encryption step, comprising: the encrypted data item; and the encrypted one or more conditions** (see Sudi col. 14, 26—29, If a recipient performs the processing required by the invention to form the phrase indicating assent to the terms and conditions, combines that phrase together with a digest of the terms and conditions themselves to form a key needed to unwrap the digital data on which he seeks to rely).

As to claim 13, the combination of Sudi and Koyama teaches **a method, wherein the step of encrypting the combination to produce a digitally signed data block uses a private key of a public/private key cryptographic solution, and wherein the method includes transmitting to**

the recipient the public key of the cryptographic solution (see Koyama par. [0022], The digital signature technique is a method of converting data by using a private key that is used in the public key cryptography. A sender who desires to transmit data containing a digital signature uses his/her own private key to convert data desired to be transmitted. Upon receipt of the data containing the digital signature, a recipient converts the data by using a public key).

As to claim 14, the combination of Sudi and Koyama teaches **a method, wherein the step of encrypting the combination to produce a digitally signed data block uses a private key of a public/private key cryptographic solution, and wherein the method includes transmitting to the recipient information for obtaining the public key of the cryptographic solution**.

As to claim 15, the combination of Sudi and Koyama teaches **a method, including compiling a set of encryption results which set includes the results of each step of encrypting, and wherein the step of transmitting includes the step of transmitting the set of encryption results to the recipient** (see Koyama, par. [0022], A sender who desires to transmit data containing a digital signature uses his/her own private key to convert data desired to be transmitted. Upon receipt of the data containing the digital signature, a recipient converts the data by using a public key. At this time, when proper data is obtained, the digital signature can be determined to be correct. This technique is enabled when only the data sender knows the private key.).

As to claim 16, the combination of Sudi and Koyama teaches **a method, including the step of transmitting to a recipient the hashed representations of the data item and conditions and the digital signature block such that a recipient, who has access to the cryptographic**

process used to perform the step of encrypting the combination and has access to a corresponding decryption key, is enabled to: decrypt the digital signature block; combine the hashed representations of the data item and conditions to generate a combined digest; and compare the decrypted signature block with the combined digest to determine whether they match (see Koyama, par. [00361], The communication unit 202 of the user terminal 201 shown in FIG. 3 receives a signal of the aforementioned data, and outputs the encrypted distribution format data 301 to the conversion unit 211. Using the private key 2 preset for the per-user in the user terminal 201, the conversion unit 211 decrypts the encrypted distribution format data 301. The determination unit 208 performs a hash conversion for the utilization restriction information 303, and compares the conversion result to the hash value 304. Thereby, the determination unit 208 verifies that the utilization restriction information 303 has not been revised. The decrypted distribution format data 301 is then stored into the storage medium 203 via the storage medium interface 204.).

As to claim 17, the combination of Sudi and Koyama teaches **a method, wherein the step of combining the hashed representations to generate a combined digest comprises the steps of: concatenating the hashed representations to generate a double digest; and hashing the double digest to generate a final combined digest** (see Sudi col. 5, lines 56—62, The various digested data (formed at P12, P16 and P20) are then combined by computer 102 using combine function 28 to form a wrap key value 30. That is, the digest of the conditions 14, the digest of the acceptance phrase 20, and, if provided, the digest of the other data 26 (or the other data 22 directly) are then combined using combine function 28 to produce a wrap key value 30 (at P22).).

As to claim 18, the combination of Sudi and Koyama teaches **a method, wherein each of a plurality of data items is separately encrypted and combined, and the combination is then further encrypted .**(see Sudi col. 7, lines 32—35, For example, the various components (conditions 10, acceptance phrase 16 and optionally other data 22) can first be combined and then their combination can be digested. This latter approach may be more cryptographically secure)

As to claim 19, the combination of Sudi and Koyama teaches **a method, generated by a method according to claim 10, comprising the following steps performed in response to receipt by the recipient of the transmitted data item, one or more conditions and the digital signature block: decrypting the digital signature block to produce a first result; encrypting the data item, encrypting the one or more conditions separately from the data item, and combining the encrypted data item and encrypted one or more conditions to produce a second result; and comparing the first and second results to determine whether they match** (see Sudi, col. 7, lines 26—35, As shown above (FIGS. 1-4), the wrap and unwrap keys are formed by first digesting the various components (conditions 10, acceptance phrase 16 and optionally other data 22) and then combining the digests. This approach is shown only be way of example, and other orders of digesting and combining are contemplated. For example, the various components (conditions 10, acceptance phrase 16 and optionally other data 22) can first be combined and then their combination can be digested. This latter approach may be more cryptographically secure).

As to independent claim 20, this claim directed to **a computer program product loadable into the internal memory of a digital computer, comprising software code portions for** executing the method of claim 1; therefore it is rejected along similar rationale.

As to independent claim 21, this claim directed to **a computer program product loadable into the internal memory of a digital computer, comprising software code portions for** executing the method of claim 19; therefore it is rejected along similar rationale.

As to claim 23, the combination of Sudi and Koyama teaches **a data processing apparatus for verifying a conditional electronic signature, generated by a method** (see Sudia col. 3, lines 39—43, In order to verify the CA's signature, the certificate content must be hashed and encrypted with the same conditions and acceptance phrase), **comprising: means for receiving the transmitted data item, one or more conditions and the digital signature block** (see Koyama par. [0021], A data transmission side can encrypt data by using the public key, and can transmit the encrypted data to the reception side); **and one or more cryptographic components for: decrypting the digital signature block to produce a first result; encrypting the data item, encrypting the one or more conditions separately from the data item, and combining the encrypted data item and encrypted one or more conditions to produce a second result; and comparing the first and second results to determine whether they match** (see Sudi, col. 7, lines 26—35, As shown above (FIGS. 1-4), the wrap and unwrap keys are formed by first digesting the various components (conditions 10, acceptance phrase 16 and optionally other data 22) and then combining the digests. This approach is shown only be way of example, and other orders of digesting and combining are contemplated. For example, the various components (conditions 10, acceptance phrase 16 and optionally other data 22) can first be combined and

then their combination can be digested. This latter approach may be more cryptographically secure)..

As to independent claim 26, this claim directed to **a computer program comprising program code instructions for controlling the operation of a data processing apparatus on which the program code** executing the method of claim 24; therefore it is rejected along similar rationale.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Ion US Pub NO.: 20020094090 A1, Wasilewski et al. US Pub. No.: 20030074565 A1, O'Donnell et al. US Patent No.: 6571335 B1.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to NEGA WOLDEMARIAM whose telephone number is (571)270-7478. The examiner can normally be reached Monday to Friday between the hours of 8:00am to 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/NEGA WOLDEMARIAM/
Examiner, Art Unit 2433

/Carl Colin/
Primary Examiner, Art Unit 2433